

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-186326

(43)Date of publication of application : 06.07.2001

(51)Int.Cl.

H04N 1/387
G06T 1/00
G09C 5/00
H04N 1/40

(21)Application number : 11-369697

(71)Applicant : RICOH CO LTD

(22)Date of filing : 27.12.1999

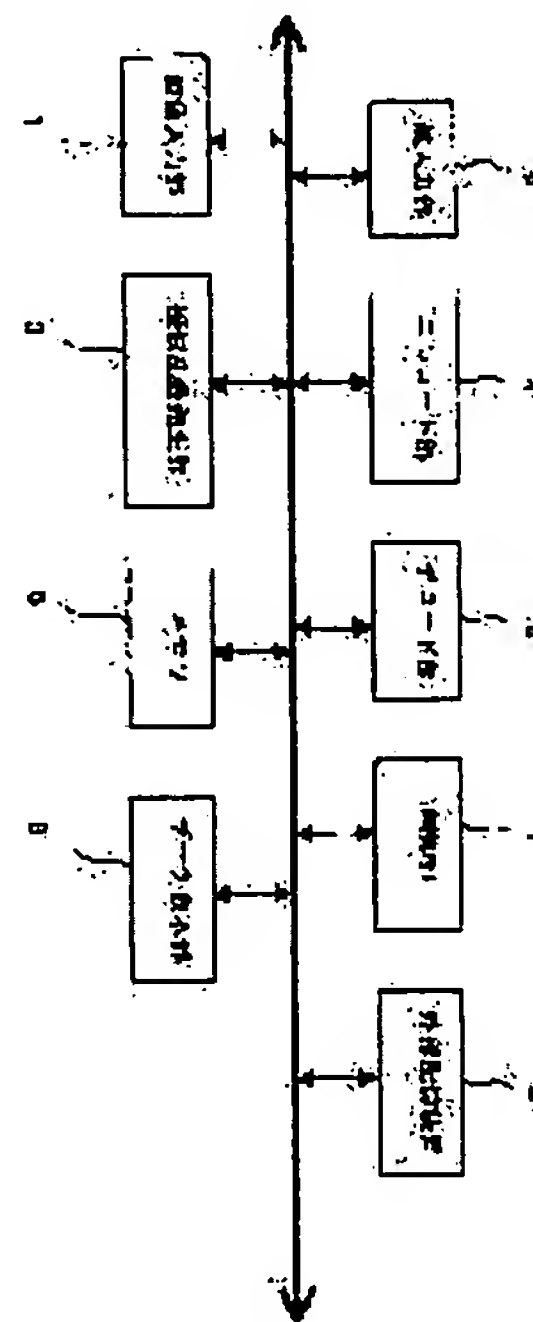
(72)Inventor : ABE TEI

(54) METHOD FOR EMBEDDING PICTURE FORGERY VERIFYING DATA, METHOD AND DEVICE FOR VERIFYING FORGERY OF PICTURE AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To verify without requiring a special picture format and to unnecessitate recording of additional information such as signature information by embedding data for verifying forgery to picture data itself, and to specify a pixel different from the original, that is a forged area, by verifying the original or not by the unit of the pixel on inspection.

SOLUTION: A random number 3 is initialized by key information 2. The respective pixel value of inputted picture data 1 and a random number are calculated to generate data for verifying forgery to embed 4 it in the picture data. On inspection, data for inspection is generated from picture data similarly to the procedure and this is compared 5 with the data for inspection embedded in the picture data, thereby forgery is decided.



LEGAL STATUS

[Date of request for examination] 13.05.2004

[Date of sending the examiner's decision of rejection] 27.12.2005

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-186326

(P 2 0 0 1 - 1 8 6 3 2 6 A)

(43) 公開日 平成13年7月6日(2001.7.6)

(51) Int. Cl. ⁷	識別記号	F I	テ-マコ-ト (参考)
H04N 1/387		H04N 1/387	5B057
G06T 1/00		G09C 5/00	5C076
G09C 5/00		G06F 15/66	B 5C077
H04N 1/40		H04N 1/40	Z 5J104

審査請求 未請求 請求項の数 6 O L (全 6 頁)

(21) 出願番号 特願平11-369697

(22) 出願日 平成11年12月27日(1999.12.27)

(71) 出願人 000006747

株式会社リコー

東京都大田区中馬込1丁目3番6号

(72) 発明者 阿部 倭

東京都大田区中馬込1丁目3番6号 株式

会社リコー内

(74) 代理人 100073760

弁理士 鈴木 誠 (外1名)

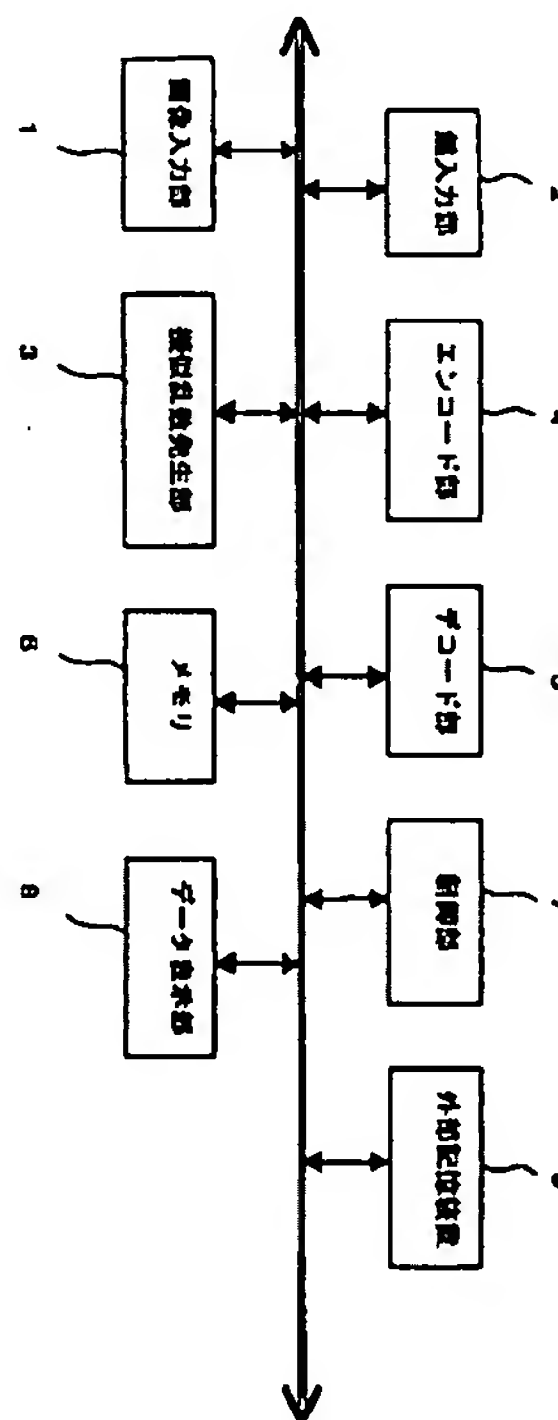
最終頁に続く

(54) 【発明の名称】 画像の改ざん検証データ埋め込み方法、画像の改ざん検証方法、画像の改ざん検証装置および記録媒体

(57) 【要約】

【課題】 画像データそのものに改ざんを検証するためのデータを埋め込むことにより、特別な画像フォーマットを用いる必要がなく、検証が可能であり、署名情報のような付加的な情報を記録する必要がなく、さらに、検証の際には画素単位で原本か否かの検証を行うことから、原本と異なる画素すなわち改ざんのあった箇所の特定が可能である。

【解決手段】 鍵情報(2)によって乱数(3)を初期化する。入力画像データ(1)の各画素値と乱数とを演算して改ざん検証用データを生成し、画像データに埋め込む(4)。検証は、上記手順と同様にして画像データから検証用データを生成し、これを画像データに埋め込まれた検証用データと比較する(5)ことにより、改ざんを判定する。



【特許請求の範囲】

【請求項 1】 デジタル画像から改ざんを検証するためのデータ（以下、検証データ）を生成し、該検証データを前記画像に非可視的に埋め込むことを特徴とする画像の改ざん検証データ埋め込み方法。

【請求項 2】 前記画像の各画素が複数ビットで表現されるとき、前記各画素毎に、所定数ビットの画素値と乱数とを用いた所定の演算によって検証データを生成し、該検証データを前記各画素の所定ビット位置に埋め込むことを特徴とする請求項 1 記載の画像の改ざん検証データ埋め込み方法。

【請求項 3】 前記画像の全ての画素に、前記検証データを埋め込むことを特徴とする請求項 1 または 2 記載の画像の改ざん検証データ埋め込み方法。

【請求項 4】 請求項 1 記載の方法によって改ざん検証データが埋め込まれた画像から所定の演算によって検証データを生成し、該生成された検証データと埋め込まれている改ざん検証データとを比較することにより前記画像が改ざんされているか否かを判定することを特徴とする画像の改ざん検証方法。

【請求項 5】 鍵情報を入力する手段と、該鍵情報を基に乱数を発生する手段と、デジタル画像と前記乱数を用いて所定の演算を行うことにより改ざん検証データを生成し、前記画像中に改ざん検証データを埋め込む手段と、改ざん検証データが埋め込まれた画像と前記乱数を用いて所定の演算を行うことにより検証データを生成し、該生成された検証データと埋め込まれている改ざん検証データとを比較することにより画像の改ざんを検証する手段とを備えたことを特徴とする画像の改ざん検証装置。

【請求項 6】 デジタル画像を入力する機能と、該デジタル画像から改ざん検証データを生成する機能と、該検証データを前記画像に非可視的に埋め込む機能と、改ざん検証データが埋め込まれた画像から所定の演算によって検証データを生成する機能と、該生成された検証データと埋め込まれている改ざん検証データとを比較することにより画像の改ざんを検証する機能をコンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、デジタル画像データに証拠性を持たせるための技術に関し、特に画像の改ざんを検証するための検証データの埋め込み方法、画像が改ざんされたか否かを判定できる画像の改ざん検証方法、画像の改ざん検証装置および画像の改ざん検証プログラムを記録した記録媒体に関し、本発明の検証方法によって、従来ではデジタル画像の偽造が容易であったために、フィルムと印画紙を用いた写真（銀鉛写真）から置き換えることができなかったような用途、分野にもデ

ジタル画像を用いることができる。

【0002】

【従来の技術】 近年、デジタルカメラやスキャナなどのデジタル画像入力機器の画質が高画質化し、普及するに伴い、従来の銀鉛写真をデジタル画像に置き換える動きが見られる。その場合に、デジタル画像データ（以下、単に「画像」、「デジタル画像」あるいは「画像データ」という）の改ざんの防止や検証の仕組みを確立することが急務となっている。

【0003】 つまり、デジタル画像データは加工や改ざんが容易であるため、デジタル画像入力機器で撮像された画像データをいくつかの経路を通して人や機関に渡された時に、それが本当に撮像された画像データそのもの（原本）であることを保証する仕組みが必要となる。

【0004】 このような目的を達成する一つの手法として電子署名が挙げられる。電子署名は一般的には、保証する対象のデータから情報（署名情報）を作成し、画像ファイルの一部もしくは他のファイルにその情報を記録しておく。検証時には画像データから署名情報を再度作成し、画像ファイルまたは他のファイルに記録されているオリジナルの署名情報と比較することによって、原本か否か（改ざんされたか否か）を判定する。

【0005】 また、特開平 11-98344 号公報に記載された「電子透かしを用いたデジタル画像の違法改ざん判定方法及び装置」には、原画像と原画像に対応する透かし画像を管理装置にそれぞれ登録しておき、不正な改ざんの疑いがある合成画像と管理装置に登録された原画像とを比較し、その差分から透かし画像を抽出し、この抽出された透かし画像と管理装置にあらかじめ登録された透かし画像とを比較し、その結果が不一致の場合には画像が改ざんされたと判定する方法も提案されている。

【0006】

【発明が解決しようとする課題】 上記した電子署名を用いた方法は、ファイルに署名情報を記録しておく必要があることから、特定のファイルフォーマットしか扱うことができず、また、検証結果として原本か否かのみの判定であり、原本でないと判定した場合に改ざん箇所を特定できない欠点がある。

【0007】 また、前掲した公報の方法では、あらかじめ原画像と原画像に対応する透かし画像を登録しておく必要があることから、実用化が難しい。

【0008】 本発明は上記した問題に鑑みてなされたものであり、本発明の目的は、画像データそのものに改ざんを検証するためのデータを埋め込むことにより、特別な画像フォーマットを用いる必要がなく、検証が可能であり、署名情報のような付加的な情報を記録する必要がなく、さらに、検証の際には画素単位で原本か否かの検証を行うことから、原本と異なる画素すなわち改ざんのあった箇所の特定が可能である、画像の改ざん検証デー

タ埋め込み方法、画像の改ざん検証方法、画像の改ざん検証装置および記録媒体を提供することにある。

【0009】

【課題を解決するための手段】本発明では、デジタル画像データの原本を、1画素も何らの変化がないものと定義し、逆に1画素でも何らかの変化があった場合に原本でない（改ざんされた）と定義する。このような定義に基づいて、デジタル画像そのものに画像から生成したデータを画像自体に埋め込み、検証の際にはその埋め込んだ情報が抽出できるか否かによって改ざんがなされたか否かの判定を行う。

【0010】本発明では、デジタル画像自体に改ざんを検証するためのデータを非可視的に埋め込むため、特別な画像フォーマットを用いる必要がなく、検証が可能である。つまり、ファイルフォーマットには依存しないため、既存のファイルフォーマットがそのまま利用できることは勿論、本発明の方式に準拠しない他の画像フォーマット読み取り装置でも通常の画像のように扱うことができる（埋め込まれた検証用のデータは通常の画像データとして無視されるのみである）。また、検証の際には検証の対象となる画像のみで検証ができることから、実施上の困難さがなく汎用性が高い。

【0011】本発明では、デジタル画像の全ての画素に対して改ざんを検証するためのデータを埋め込むため、画素毎に改ざんされたか否かの検証が可能となり、どの1画素を改ざんしても改ざんの検知ができることから、改ざんの位置までも検証者に提示できる。

【0012】本発明では、改ざんを検証するためのデータを各画素の最下位ビットに埋め込むため非可視性に優れ、改ざん検証用のデータが埋め込まれていることは知覚できない。従って、画像を原画像とほぼ同じ状態に保つことができるため、本発明を適用することによる画像の劣化がなく、秘匿性に優れる。

【0013】本発明では、改ざんを検証するためのデータを画素値と鍵情報で初期化した擬似乱数を用いて計算するため、画像固有の情報となっていること、鍵情報で擬似乱数が初期化されているため、鍵情報がなければ同じ擬似乱数は発生できないことから安全性に優れている。すなわち、この鍵情報を知らない者が改ざんを施した後で改ざん検証用のデータを上書きして改ざんがなかったように加工することが不可能である。

【0014】さらに、本発明では、画像データを損なうことなく、非可視的に改ざん検証用のデータを埋め込むことができ、改ざんの検証を確実に行うことができる。

【0015】

【発明の実施の形態】以下、本発明の一実施例を図面を用いて具体的に説明する。本発明はデジタル画像データの種類（2値、多値、カラー、動画など）によらず適用が可能であるが、ここでは多値画像（1画素あたり8ビットを用いて表現）に適用した場合を例に説明する。

【0016】図1は、本発明の実施例に係る画像処理装置の構成を示す。この画像処理装置は、デジタル画像データを本装置内に取り込む画像入力部1、鍵情報を入力する鍵入力部2、擬似乱数を発生する擬似乱数発生部3、改ざん検証データの埋め込み処理（エンコード処理）を行うエンコード部4、画像の改ざん検証処理（デコード処理）を行うデコード部5、画像データや処理結果などを蓄えておくメモリ6、各種制御を行う制御部7、画像データなどを表示するデータ表示部8、情報記憶媒体を駆動する外部情報記憶装置9から構成される。

【0017】図2は、改ざん検証用データの埋め込み（エンコード）処理のフローチャートを示す。図2を用いてエンコード処理についてステップ毎に説明する。

【0018】画像入力部1によりデジタル画像データを入力する（ステップ101）。次いで、鍵入力部2から鍵情報を入力する（ステップ102）。擬似乱数発生部3では、乱数を、ステップ102で入力した鍵情報に基づいて初期化する（ステップ103）。

【0019】エンコード部4は、注目画素の画素値（8ビットのデータ）を得る（ステップ104）。続いて、擬似乱数発生部3は鍵情報で初期化された乱数を発生する（ステップ105）。エンコード部4は、画素値の上位7ビットとステップ105の処理で発生した乱数から、改ざん検証用のデータ（1ビット）を計算する（ステップ106）。

【0020】図3は、改ざん検証用データを生成して埋め込む処理を説明する図である。画像データの上位7ビットと乱数とを用いて所定の演算を行って1ビットの検証用データを生成し、画像データの最下位ビットを、検証用データで置き換える。

【0021】乱数 r は任意のビット数でよいが、ここでは1ビットとして説明する。図3に示すようにビット値を定義すると、関数 F の一例として、 b_1 から順に r を含めて全てのビットについて排他的論理和を演算することで、1ビットの改ざん検証用データ（ b_8 ）を生成できる。すなわち、

$$c_1 = b_1 \oplus b_2$$

$$c_2 = c_1 \oplus b_3$$

$$c_3 = c_2 \oplus b_4$$

$$c_4 = c_3 \oplus b_5$$

$$c_5 = c_4 \oplus b_6$$

$$c_6 = c_5 \oplus b_7$$

$$b_8 = c_6 \oplus r$$

ここで、 \oplus は排他的論理和を示す。一つの式で表せば次のようになる。

$$b_8 = (((((b_1 \oplus b_2) \oplus b_3) \oplus b_4) \oplus b_5) \oplus b_6) \oplus b_7) \oplus r$$

上記した処理では r が1ビットとして説明したが、 r が任意のビット数をとる場合には、そのビット数分だけ排他的論理和演算を繰り返せばよい。また、 $b_1 \sim b_7$ の

上位7ビットの全てを用いて演算したが、全てではなく所定のビット位置を選択して用いるようにしてもよい。ただし、この場合は固定のビット位置（例えば常にb3とb5）を用いるよりは、乱数を使って、選択するビット位置を変更させる。これにより、セキュリティレベルが一層向上することになる。

【0022】エンコード部4は、ステップ106で計算した改ざん検証用のデータで画素値の最下位ビット値を置き換える（ステップ107）。制御部7は、全ての画素の処理を終えたか否かを判定し（ステップ108）、
10 全ての画素の処理を終えたらエンコード処理を終了し、未処理の画素があれば注目画素を1画素ずらし、処理ステップ104に進む。

【0023】以上のようにして、画像の全ての画素に改ざん検証データを埋め込むことができる。なお、画質が劣化しない範囲であれば、埋め込む位置は他のビット位置でもよく、また埋め込むビット数は複数ビットでもよい。

【0024】図4は、改ざん検証（デコード）処理のフローチャートを示す。図4を用いてデコード処理につい
20 てステップ毎に説明する。

【0025】画像入力部1によりデジタル画像データを入力する（ステップ201）。鍵入力部2から鍵情報を入力する（ステップ202）。次いで、擬似乱数発生部3では、乱数を、ステップ202で入力した鍵情報に基づいて初期化する（ステップ203）。これにより、エンコード時の鍵情報と同一の鍵情報が入力されなければ、エンコード時と同じ乱数が発生しないことになる。

【0026】デコード部5では、注目画素の画素値（8ビットのデータ）を得る（ステップ204）。続いて、
30 擬似乱数発生部3は鍵情報で初期化された乱数を発生する（ステップ205）。デコード部5では、画素値の上位7ビットとステップ205で発生した乱数から、改ざん検証用のデータ（1ビット）を計算する（ステップ206）。デコード部5では、ステップ206で計算した改ざん検証用のデータと画素値の最下位ビット値を比較し、一致するならステップ209へ進み、一致しないなら処理ステップ208へ進む。

【0027】一致しないときデコード部5は、注目画素を改ざんされた画素として記録し（ステップ208）、
40 全画素を通して一度でもステップ208を通ったなら、画像データに改ざんがあったと判定する。

【0028】制御部7は、全ての画素の処理を終えたか否かを判定し（ステップ209）、全ての画素の処理を終えたらエンコード処理を終了し、未処理の画素があれば注目画素を1画素ずらし、ステップ204に進む。

【0029】なお、図1の構成は一例であって、例えば画像入力部1、鍵入力部2、擬似乱数発生部3、エンコ

ード部4、メモリ6、制御部7、データ表示部8、外部記憶装置9からなるエンコード装置を送信側に設け、一方、画像入力部1、鍵入力部2、擬似乱数発生部3、デコード部5、メモリ6、制御部7、データ表示部8、外部記憶装置9からなるデコード装置を受信側に設け、送信側と受信側をネットワークで接続する構成を採るようにしてもよい。

【0030】図5は、本発明をソフトウェアによって実現する場合のシステム構成例を示す。CD-ROMなどの記録媒体には、本発明の画像の改ざん検証処理プログラムが記録されていて、これをシステムにインストールする。スキャナから読み込まれた画像あるいはシステム内に蓄積されている画像に対して、改ざん検証データを埋め込み、この画像データを他の媒体に出力したり、あるいはネットワークを介して他の装置に伝送する。また、システムに取り込まれた、改ざん検証データが埋め込まれている画像データから、正しく検証データが復元されたときは改ざんされていない真正な画像であると判定する。

【0031】

【発明の効果】以上、説明したように、本発明によれば種々の画像データに対して、改ざん検証用のデータを非可視的に埋め込むことによって、改ざんの有無を判定することが可能となる。特に、検証の際に原画像を必要とせず、検証の対象となる画像のみで検証が可能であり、既存の画像ファイルフォーマットをそのまま利用でき、また改ざんの位置を特定することができる。さらには、処理量が非常に少なく実現性に優れていて、従来では困難であったデジタル画像データの検証を確実にかつ簡便に行うことができる。

【図面の簡単な説明】

【図1】本発明の実施例の構成を示す。

【図2】エンコード処理のフローチャートを示す。

【図3】改ざん検証用データの埋め込みを説明する図である。

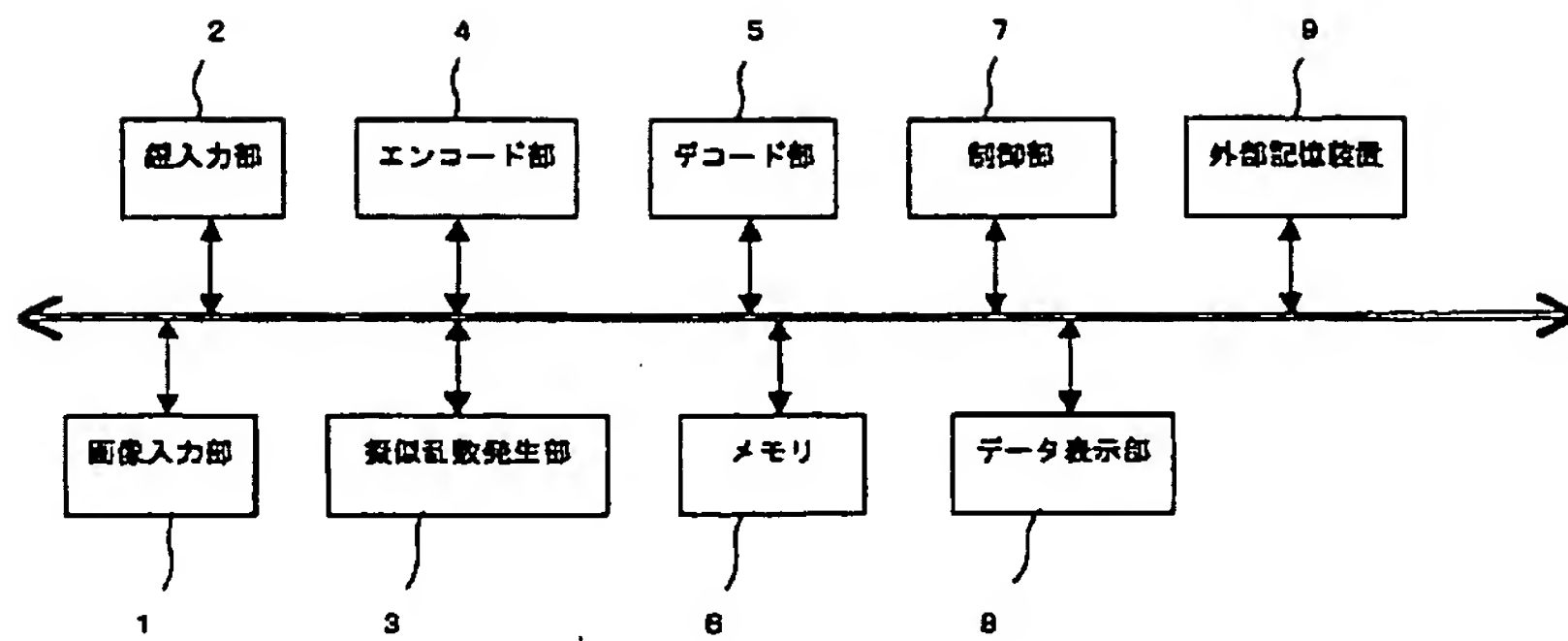
【図4】デコード処理のフローチャートを示す。

【図5】本発明をソフトウェアによって実現する場合の構成例を示す。

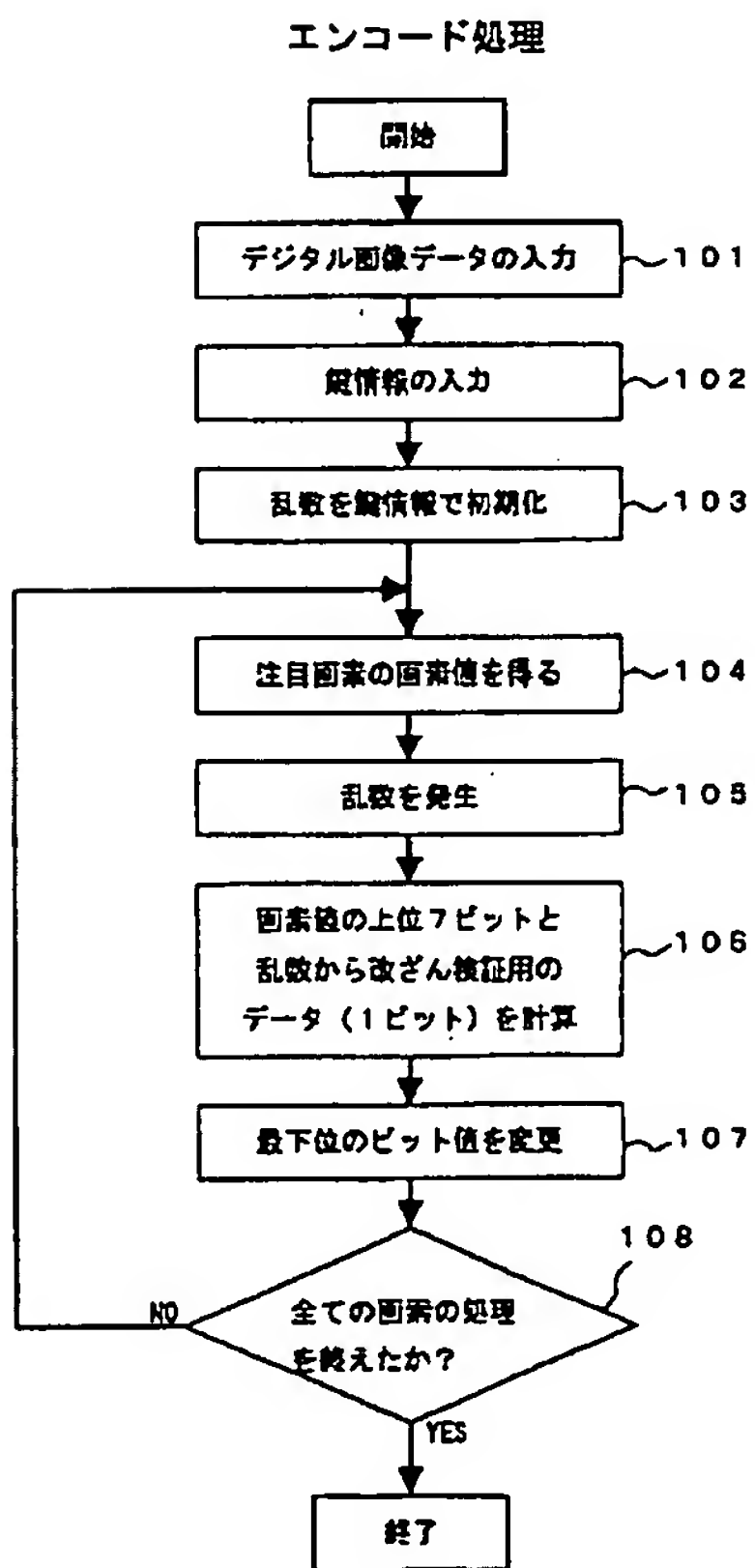
【符号の説明】

- 1 画像入力部
- 2 鍵入力部
- 3 擬似乱数発生部
- 4 エンコード部
- 5 デコード部
- 6 メモリ
- 7 制御部
- 8 データ表示部
- 9 外部記憶装置

【図 1】

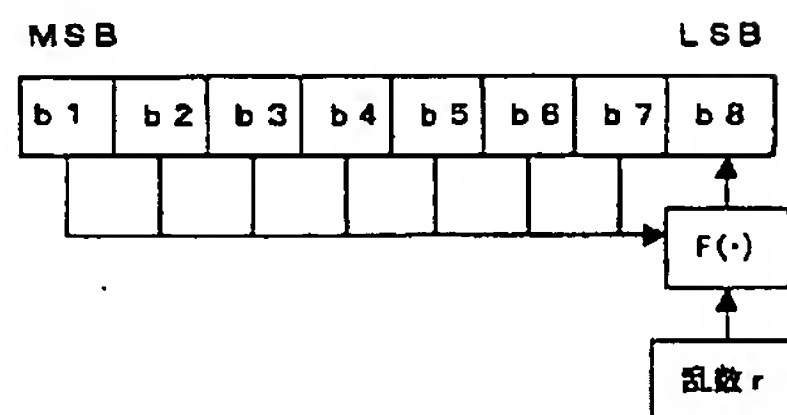


【図 2】

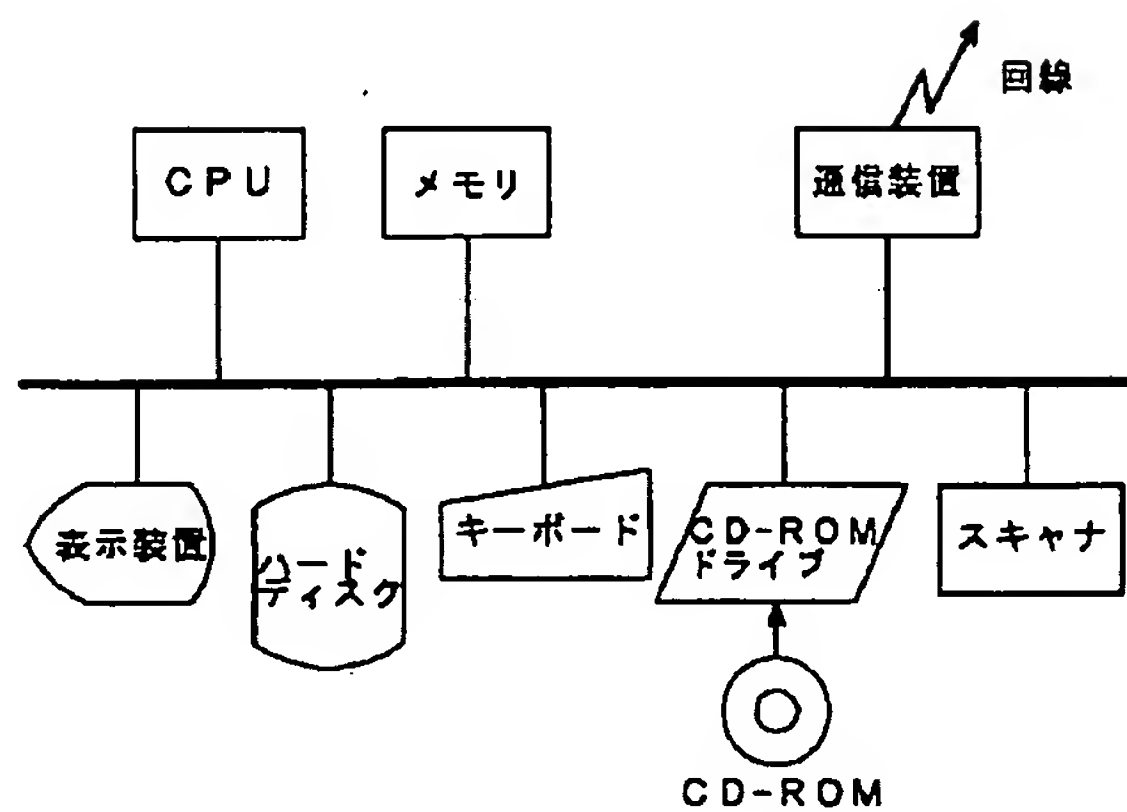


【図 3】

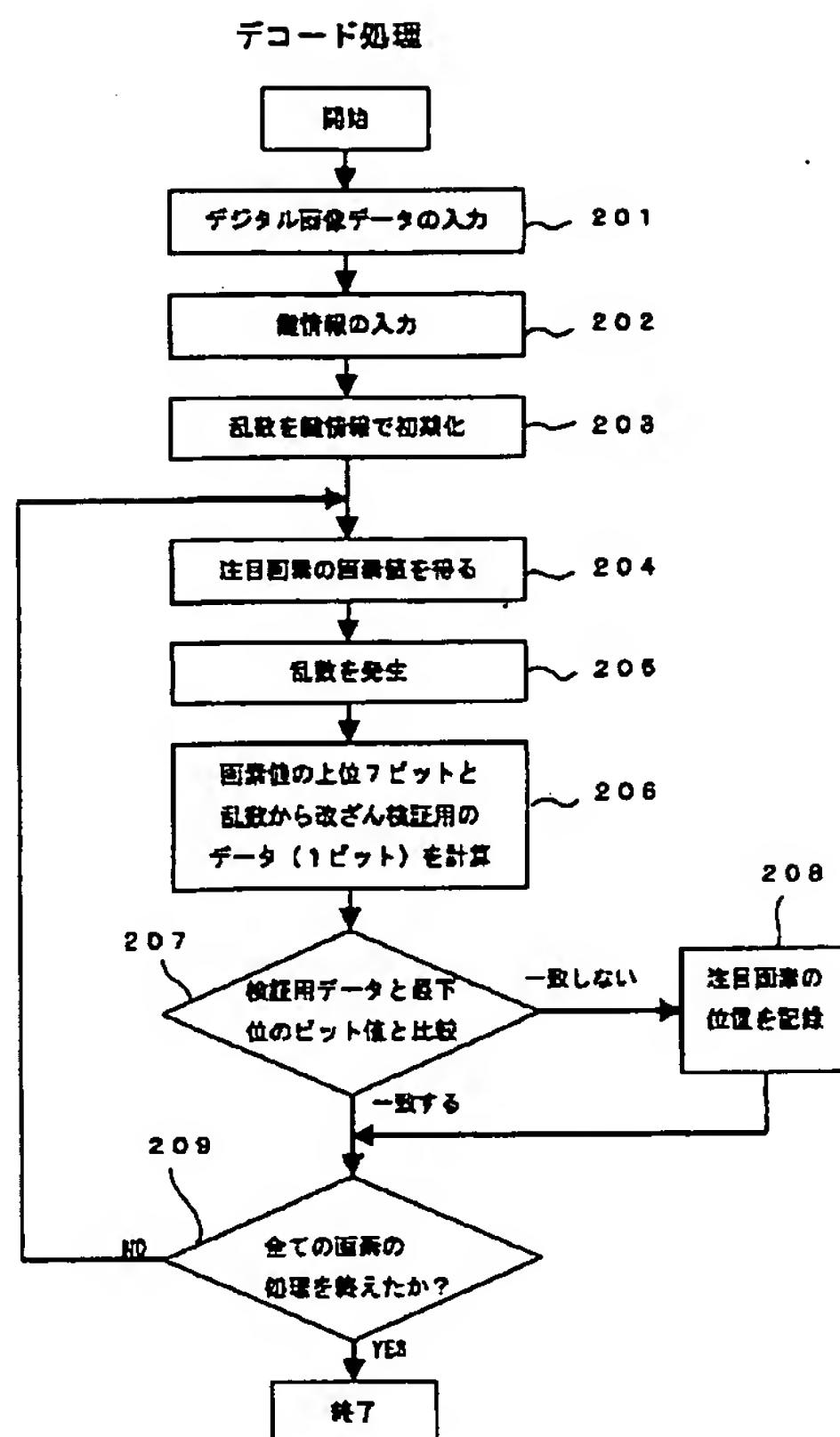
改ざん検証用データの埋め込み



【図 5】



【図 4】



フロントページの続き

Fターム(参考) 5B057 AA11 BA24 CA16 CA19 CB16
 CB19 CC02 CE08 CH07 CH11
 DA02 DA08 DA16
 5C076 AA14 BA02 BA03 BA04 BA07
 CA08
 5C077 LL14 NN04 PP19 PP23 PQ12
 PQ22 SS02
 5J104 AA08 CA04 FA07 LA01 PA14